Cyberspace, Information Strategy, and International Security

Bibliography

February 2018

CGSR

Center for Global Security Research

LAWRENCE LIVERMORE NATIONAL LABORATORY

Bibliography for Workshop
Cyberspace, Information Strategy, and International Security

Center for Global Security Research, Lawrence Livermore National Laboratory
February 27-28, 2018

Jaclyn A. Kerr

Key questions posed for the workshop:

1. How might increasingly competitive information strategies and military uses of cyberspace affect the security of the United States and its allies?
2. Who are the stakeholders in cyberspace security and what interests will shape their future choices?
3. What can be done to mitigate risks?

The list of readings below provides some overview and background for the topics covered in the workshop. This includes some materials shared by workshop participants. While some references are to books or materials not available online, where possible references include links to accessible versions of articles.

Panel 1: Cyberspace and Security: Complexities of the Cyber Domain

This panel will address:

- How has the cybersecurity problem evolved in U.S. defense strategy over the last two decades?
- How might it yet evolve? What are the main challenges ahead?
- How is military competition in this area affected by the unique characteristics of the cyber domain (i.e. dual use technologies, attribution challenges, multiplicity of actors)? How can we understand the relationship between the cyber domain and civilian cyberspace?

The following books provide valuable overall references regarding the history and ongoing development of "Cyberspace," cybersecurity, and military cyber conflict:

<u>On Internet History and Governance:</u>

- Abbate, Janet. *Inventing the Internet*. 1st edition. Cambridge, Mass: The MIT Press, 1999.

- DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.
- Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. 1 edition. New York: Oxford University Press, 2006.
- Lessig, Lawrence. *Code: And Other Laws of Cyberspace*. New York: Basic Books, 1999.
- Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. 1st edition. Cambridge, Mass.: The MIT Press, 2010.
- Zittrain, Jonathan. *The Future of the Internet--And How to Stop It*. First Edition. New Haven Conn.: Yale University Press, 2008.

On Cyber Conflict:

- Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.
- Kaplan, Fred. *Dark territory: The secret history of cyber war*. Simon and Schuster, 2016.
- Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. Penguin, 2017.
- Valeriano, Brandon, and Ryan C. Maness. *Cyber war versus cyber realities: cyber conflict in the international system*. Oxford University Press, USA, 2015.

Panel 2: Cyberspace in the Strategies of Potential Adversaries

This panel will address:

- How do Russia and China think about and operate in cyberspace to contest U.S. power and interests? Do they make distinctions for different types of conflicts?
- How effective are these strategies and how might they develop further?
- What other actors pose the most serious threats in cyberspace now and in the future?

On China:

Kania, Elsa B., and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *Cyber Defense Review*, Winter 2018.

Kania, Elsa, Samm Sacks, Paul Triolo and Graham Webster. "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated." New America Foundation Cybersecurity Initiative, September 2017. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review*, 111, 3, 2017: 484-501. https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf

Lindsay, Jon, Tai Ming Cheung, and Derek Reveron, Editors. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, 2015.
Segal, Adam. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Hoover Institution, June* 2 (2017).
https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf

Triolo, Paul, Samm Sacks, Graham Webster and Rogier Creemers. "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework." New America Foundation Cybersecurity Initiative, November 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/

On Russia:
Adamsky, Dmitry. *Cross-domain coercion: The current Russian art of strategy*. IFRI Security Studies Center, 2015. https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

Disinformation: A Primer in Russian Active Measures and Influence Campaigns. Select Committee on Intelligence , United States Senate, One Hundred Fifteenth Congress, First Session. March 30, 2017. https://www.hsdl.org/?view&did=802222

Fedor, Julie and Rolf Fredheim. "We need more clips about Putin, and lots of them: Russia's state-commissioned online visual culture," Nationalities Papers, 45:2, 2017: 161-181. https://doi.org/10.1080/00905992.2016.1266608

Giles, Keir. *Handbook of Russian information warfare*. NATO Defence College Research Division, 2016. http://www.ndc.nato.int/news/news.php?icode=995

Shackelford, Scott J., Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan, and Brian Micic. "From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It." *Neb. L. Rev.* 96 (2017): 320.https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3118&context=nlr

Soldatov, Andrei and Irina Borogan. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. PublicAffairs, 2015.

On Iran and North Korea:
Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: exporting instability through cyberspace." (2015).
https://www.eastwestcenter.org/system/tdf/private/api117.pdf?file=1%26type=node%26id=35164

Herr, Trey, and Laura K. Bate. "The Iranian Cyberthreat Is Real." Foreign Policy, July 2017.
http://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real/

Panel 3: Cyberspace in the Strategies of the United States and its Allies

This panel will address:

- In U.S. military strategy, how are cyber capabilities expected to contribute to the achievement of U.S. objectives in peacetime, crisis, and war?
- How has this evolved over the last two decades and what challenges lie ahead?
- How have NATO and U.S. allies in East Asia approached security challenges in cyberspace?

United States Department of Defense, "The DOD Cyber Strategy," 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Shea, Jamie. "NATO: Stepping up its game in cyber defence." *Cyber Security: A Peer-Reviewed Journal* 1, no. 2 (2017): 165-174.

Hammock, C. J. "Enabling the Development and Deployment of NATO Cyber Operations: An Analysis of Modern Cyber Warfare Operations and Thresholds of Global Conflict." *Journal of Information Warfare* 16, no. 3 (2017): 79-94.

Kallender, Paul, and Christopher W. Hughes. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace." *Journal of Strategic Studies* 40, no. 1-2 (2017): 118-145.

Panel 4: Cybersecurity, Deterrence, and Strategic Stability

This panel will address:

- How has the cybersecurity problem evolved in U.S. defense strategy over the last two decades?
- How might it yet evolve? What are the main challenges ahead?
- How is military competition in this area affected by the unique characteristics of the cyber domain (i.e. dual use technologies, attribution challenges, multiplicity of actors)? How can we understand the relationship between the cyber domain and civilian cyberspace?

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press, 2017.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." Orbis 61, no. 3, 2017: 381-393.

Jasper, Scott. “Implementing Automated Cyber Defense.” United States Cybersecurity Magazine, Winter 2018: 22-25.

Kreps, Sarah E., and Jacquelyn Schneider. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics." (2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3104014

Lindsay, Jon & Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," 2016, http://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf

Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3, 2017: 44-71. https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf

Rid, Thomas & Ben Buchanan, "Attributing Cyber Attacks," https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf

Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 72-109. https://cornell.app.box.com/s/58xm5d4xwbdjq549vx5xnwc3qu1dqybk

Schneider, Jacquelyn. “Deterrence in and Through Cyberspace.” 2018. http://deterrence.ucsd.edu/_files/CDD_Intro_v2.pdf

Panel 5: Information Warfare Present and Future

This panel will address:

- How should we think about strategic uses of information through cyberspace beyond the traditional understanding of cyber operations? How might this evolve in the future?
- How do cyberspace- and information-related security concerns and vulnerabilities of democratic and authoritarian states differ and how has this impacted their approaches to cyberspace?
- What approaches are currently being taken or should be taken by the U.S. and its allies to safeguard against or deter information and influence campaigns? What are the risks of addressing such problems as military concerns in democracies?

Lin, Herbert and Jaclyn Kerr. “On Cyber - Enabled Information/Influence Warfare and Manipulation.” *Oxford Handbook of Cyber Security*. Ed. Paul Cornish. Oxford: Oxford University Press, 2018 (forthcoming). https://cisac.fsi.stanford.edu/sites/default/files/cyber-enabled_influence_warfare-ssrn-v1.pdf

Powers, Shawn, and Markos Kounalakis, editors. “Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation.” Advisory Commission on Public Diplomacy, U.S. Department of State, May 2017. https://www.state.gov/documents/organization/271028.pdf
Starbird, Kate. "Examining the Alternative Media Ecosystem Through the Production of Alternative Narratives of Mass Shooting Events on Twitter." In *ICWSM*, pp. 230-239. 2017.

Wanless, Alicia and Berk, Michael. A Particiaptory Propaganda Model. Conference proceedings Social Media and Social Order. Oslo, December 2017. https://lageneralista.com/wp-content/uploads/2018/01/A-Participatory-Propaganda-Model-.pdf

Woolley, Samuel C., and Philip N. Howard. "Computational propaganda worldwide: Executive summary." (2017). http://275rzy1ul4252pt1hv2dqyuf.wpengine.netdna-cdn.com/wp-content/uploads/2017/07/Casestudies-ExecutiveSummary-1.pdf

Panel 6: Roles of the Private Sector and Other Stakeholders

This panel will address:

- How are cyber- and informational-conflict changing the nature of civilian cyberspace (including technical and governance structures of the Internet)? How significant are these changes in an historical perspective?
- To what extent are the security concerns of stakeholders at odds and where do they converge?
- How successful are current approaches in balancing values and interests? Are further innovations needed?

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore et al. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* 1, no. 1 (2015): 69-79. https://academic.oup.com/cybersecurity/article/1/1/69/2367066

Herr, Trey and Bruce Schneier, and Christopher Morris. “Taking Stock: Estimating Vulnerability Rediscovery,” Belfer Cyber Security Project White Paper Series, March 2017. https://ssrn.com/abstract=2928758
Kuehn, Andreas and Bruce McConnell. “Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions.” EastWest Institute, February 2018. https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf?dm_i=439P,3GU,17MEK,87B,1

Nye, Joseph. "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, May 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Moussouris, Katie. "Serious progress made on the Wassenaar Arrangement for global cybersecurity," The Hill, December 2017. http://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global

Microsoft Policy Papers. "A Digital Geneva Convention to protect cyberspace," 2017. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

Mueller, Milton. "Is cybersecurity eating internet governance? Causes and consequences of alternative framings", *Digital Policy, Regulation and Governance*, Vol. 19 Issue 6, 2017: pp.415-428. https://doi.org/10.1108/DPRG-05-2017-0025

Panel 7: The Roles of Laws, Norms, and Limits in Constraining Cyber Anarchy

This panel will address:

- What roles, if any, can international law, agreed upon rules, or emergent norms play in constraining cyber behavior and arms development?
- Are there any behaviors parties might agree should be off limits?
- What lessons can be learned from recent efforts or from experience in related domains?

Donahoe, Eileen, Melissa Hathaway, Paul Twomey, James A. Lewis, Joseph Nye Jr, and Eneken Tikk. "Getting beyond Norms: New Approaches to International Cyber Security Challenges." (2017). https://www.cigionline.org/sites/default/files/documents/Getting%20Beyond%20Norms.pdf

Hollis, Duncan, and Matthew Waxman. "Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)," 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082907

Lin, Herb. "Governance of Information Technology and Cyber Weapons" from edited volume Governance of Dual-Use Technologies https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/GNF_Dual-Use-Technology.pdf

Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-746680